



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11143833 A**(43) Date of publication of application: **28 . 05 . 99**

(51) Int. Cl. **G06F 15/00**  
**G09C 1/00**  
**H04L 9/32**

(21) Application number: **09313390**(71) Applicant: **TOSHIBA CORP**(22) Date of filing: **14 . 11 . 97**(72) Inventor: **YAMADA KOUKI**

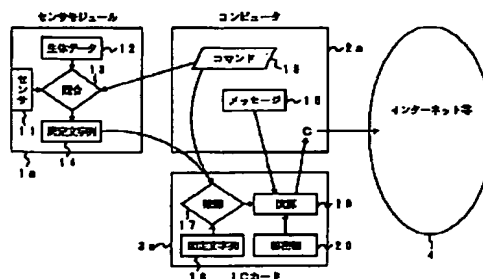
(54) **USER CONFIRMATION SYSTEM AND IC CARD  
 BY BIOLOGICAL DATA AND STORAGE MEDIUM**

COPYRIGHT: (C)1999,JPO

(57) Abstract:

**PROBLEM TO BE SOLVED:** To make it possible to protect biological data with high safety by putting them in a management range at hand of a user and to reduce a feeling of resistance and a risk of leakage of the biological data.

**SOLUTION:** This user confirmation system consists of a sensor 11 for performing a biological measurement, a biological data holding part 12 for holding biological data, a tamper proof sensor module 1a that is equipped with a collating calculation part 13 which collates measurement information measured by the sensor with the biological data in the biological data holding part and outputs a notification of the fact when a person concerned is confirmed by the collated result, an IC card 3a that performs a data output by corresponding to that a user confirmation is made when the notification is received, a confirmation processing part 17, an operation processing part 19 and a communication means 2a for performing a communication between the sensor module and the IC card.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-143833

(43)公開日 平成11年(1999) 5月28日

(51)Int.Cl. <sup>a</sup>	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 F
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 A
H 0 4 L 9/32		H 0 4 L 9/00 6 7 3 D

審査請求 未請求 請求項の数15 O L (全 22 頁)

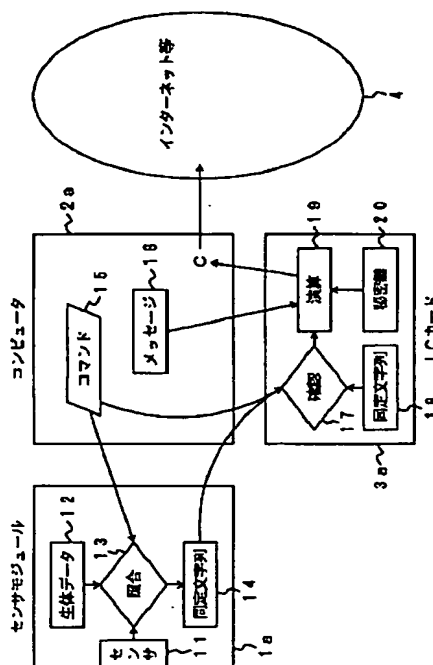
(21)出願番号	特願平9-313390	(71)出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22)出願日	平成9年(1997)11月14日	(72)発明者	山田 貢己 東京都府中市東芝町1番地 株式会社東芝 府中工場内
		(74)代理人	弁理士 鈴江 武彦 (外6名)

(54)【発明の名称】 生体データによるユーザ確認システム及びICカード並びに記録媒体

(57)【要約】

【課題】 生体データを高い安全性をもってユーザ手元の管理範囲に置いて守ることができ、ユーザの抵抗感及び生体データの漏洩危険性を低減する。

【解決手段】 生体測定を行うセンサ11、生体データを保持する生体データ保持部12、並びに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部13を備えた耐タンパー性のセンサモジュール1aと、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するICカード3a、17、19と、センサモジュールとICカードとの間の通信を行う通信手段2aとからなる生体データによるユーザ確認システム。



## 【特許請求の範囲】

【請求項 1】 生体測定を行うセンサ、生体データを保持する生体データ保持部、並びに、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えた耐タンパー性のセンサモジュールと、  
前記通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する IC カードと、  
前記センサモジュールと前記 IC カードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項 2】 生体測定を行うセンサを備えたセンサモジュールと、  
生体データを保持する生体データ保持部、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部、  
並びに、前記通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性の IC カードと、  
前記センサモジュールと前記 IC カードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項 3】 生体測定を行うセンサ、暗号化された生体データを受信しこれを復号化する復号部、並びに、前記センサにより測定された測定情報と復号化された前記生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたセンサモジュールと、  
前記暗号化された生体データを保持するとともに、当該暗号化された生体データを前記センサモジュールに送出する生体データ保持部、並びに、前記照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性の IC カードと、  
前記センサモジュールと前記 IC カードとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項 4】 前記センサモジュールに耐タンパー性を持たせたことを特徴とする請求項 3 記載の生体データによるユーザ確認システム。

【請求項 5】 生体測定を行うセンサを備えたセンサモジュールと、  
暗号化された生体データを受信しこれを復号化する復号部、並びに、前記センサにより測定された測定情報と復号化された前記生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたコンピュータと、  
前記暗号化された生体データを保持するとともに、当該

暗号化された生体データを前記コンピュータに送出する生体データ保持部、並びに、前記照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性の IC カードと、

前記センサモジュールと前記 IC カードと前記コンピュータとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項 6】 前記 IC カードはユーザ本人のデジタル署名を行う署名手段を備え、前記ユーザ確認がされたことに対応してなされるデータ出力には、前記署名手段によるデジタル署名が含まれることを特徴とする請求項 1 乃至 5 のうち何れか 1 項記載の生体データによるユーザ確認システム。

【請求項 7】 生体測定を行うセンサを備えたセンサモジュールと、

ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持部、並びに、前記ユーザ要求及び前記ログオンパスワードが入力されたときに前記生体データ保持部の生体データを前記ログオンパスワードにより復号化するとともに、この復号化された生体データと前記センサにより測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、前記ユーザ要求を実施すべき旨の通知を出力する照合計算部を備えたコンピュータと、

前記コンピュータと前記センサモジュールとの間の通信を行う通信手段とからなることを特徴とする生体データによるユーザ確認システム。

【請求項 8】 生体測定を行うセンサと、コンピュータと、IC カードとからなり、ユーザ確認を行うとともにデータの暗号化処理を行うユーザ確認システムにおいて、

前記 IC カードは、耐タンパー性を有し、かつ、生体データを保持する生体データ保持部、前記データの暗号化処理におけるその一部処理を実行する第 1 の暗号計算部、並びに、前記第 1 の暗号計算部での処理に用いられる暗号鍵を保持する暗号鍵保持部を少なくとも備えており、

前記コンピュータは、ユーザ確認通知を受けると前記データの暗号化処理における他の処理を実行する第 2 の暗号計算部を少なくとも備えており、

さらに、前記センサにより測定された測定情報と前記生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときには前記第 2 の暗号計算部に前記ユーザ確認通知を出力する照合計算手段と、

前記センサと前記 IC カードと前記コンピュータとの間の通信を行う通信手段とからなることを特徴とする生体

データによるユーザ確認システム。

【請求項9】 コンピュータに、ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持機能と、

前記ユーザ要求及び前記ログオンパスワードが入力されたときに前記生体データを前記ログオンパスワードにより復号化するとともに、この復号化された生体データと生体測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、前記ユーザ要求を実施すべき旨の通知を出力する照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項10】 コンピュータに、ユーザ確認通知を受けた場合には、データの暗号化処理における一部処理を実行するとともに、このデータ暗号化処理における他の処理の処理結果を外部から受け取り、その処理結果を前記一部処理が用いて暗号化処理を完成させる暗号計算機能と、生体測定された測定情報とユーザ確認用の生体データとを照合するとともに、照合結果よりユーザ本人と確認されたときには前記暗号計算機能に前記ユーザ確認通知を行う照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項11】 暗号化された生体データを保持するとともに、この暗号化された生体データを外部装置に出力する生体データ保持手段と、前記生体データと生体測定された測定情報とによりユーザ本人と確認された旨の照合結果を前記外部装置から通知されると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理手段とを備え、かつ耐タンバー性を有することを特徴とするICカード。

【請求項12】 前記外部装置は、生体測定を行うセンサを有するセンサモジュールであることを特徴とする請求項11記載のICカード。

【請求項13】 前記外部装置は、コンピュータであることを特徴とする請求項11記載のICカード。

【請求項14】 前記演算処理手段はユーザ本人のデジタル署名を行う署名手段を備え、前記ユーザ確認がされたことに対応してなされるデータ出力には、前記署名手段によるデジタル署名が含まれることを特徴とする請求項11乃至13のうち何れか1項記載のICカード。

【請求項15】 生体データを保持するとともに、この生体データを用いてユーザ確認を行う外部装置に前記生体データを出力する生体データ保持手段と、

データの暗号化処理における一部処理を暗号鍵を用いて実行するとともに、このデータの暗号化処理における他の処理を行う外部装置に前記一部処理の処理結果を出力する暗号計算手段と、

前記暗号鍵を保持する暗号鍵保持手段とを備え、かつ耐タンバー性を有することを特徴とするICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ICカードを利用したデジタル署名処理や、計算機ソフトウェアの使用権限確認、あるいはデータ暗号化処理の使用権限確認等を便利且つ安全に行うための生体データによるユーザ確認システム及びICカード並びに記録媒体に関する。

【0002】

【従来の技術】従来からユーザを確認するのにクレジットカードや入退室管理カード等、主に磁気カードが使われている。これに対し、最近、カードの偽造や情報漏洩を防ぐ効果等を期待して、半導体チップを内蔵した高セキュリティで高性能のICカードが使われ始めている。

【0003】しかしながら、ICカードを利用しても、紛失や盗難により他人に不正使用されたり、紛失と偽って不正使用することに対して、それを防ぐことが難しい。

20 【0004】ICカードに対応したパスワードを登録することにより不正使用を減らそうとすることが行われているが、パスワードは記憶することが煩わしく、忘れてしまう危険性や、メモを他人に読まれたりして漏洩する危険性があり、決して便利であるとは言えない。

【0005】最近では、指紋や掌型のような生体データを測定して本人を確認する技術であるバイオメトリクスとICカードとを組み合わせて入退室管理やアクセス制御を行おうとする動きがある。これによって、カードの紛失、盗難、漏洩、忘却等により生じる各種問題は解決すると思われる。

30 【0006】しかし、一方でパスワードのような自由に創造できるものではなく唯一無二の自分の身体の情報（生体データ）がどこかに登録されているということに対するユーザの抵抗感や、それが漏洩したときにパスワードのような変更が効かないという弱点及び漏洩トラブルに対するユーザの不安感が根強く残っている。したがって、バイオメトリクスをユーザ確認に用いる場合には、上記抵抗感が少なくなるような技術を提案し、また、生体データの漏洩を効果的に防止できるシステムを構築する必要がある。

40 【0007】さらに、通常ICカードを用いないことの多い計算機ソフトウェアの使用権限確認を行う環境においては、生体データを安全に保持する媒体が無く、バイオメトリクスを利用する場合には生体データを計算機の記憶媒体上に格納するしかない。しかし、この場合にはリバースエンジニアリングによって生体データが漏洩する危険性がある。

【0008】

50 【発明が解決しようとする課題】上述したように、従来のICカードとパスワードを併用する技術では、煩わし

さ、忘却あるいは漏洩の危険性といった問題点がある。

【0009】また、ICカードとバイオメトリクスの併用では、自分の身体の情報（生体データ）が登録されることへの抵抗感や、生体データが第三者へ漏洩する危険性が残っている。

【0010】さらに、ICカードを用いない環境においてバイオメトリクスを利用して使用権限の確認をする場合には、生体データを安全に記録する方法が無かった。

【0011】本発明は、上記事情を考慮してなされたもので、生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感及び生体データの漏洩危険性を低減することを可能とし、さらに使用上の煩わしさが少なくユーザ確認の確実性が高い生体データによるユーザ確認システム及びICカード並びに記録媒体を提供することを目的とする。

【0012】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、生体測定を行うセンサ、生体データを保持する生体データ保持部、並びに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えた耐タンパー性のセンサモジュールと、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行するICカードと、センサモジュールとICカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0013】本発明はこのような手段を設けたので、生体データ保持部内の生体データが耐タンパー性のセンサモジュールに保護され、生体データを高い安全性でもって守ることができ、生体データの漏洩危険性を低減するとともに、さらに使用上の煩わしさを少なくしユーザ本人確認の確実性を高くすることができる。

【0014】次に、請求項2に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、生体データを保持する生体データ保持部、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部、並びに、通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のICカードと、センサモジュールとICカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0015】本発明はこのような手段を設けたので、請求項1に対応する発明と同様な効果が得られる他、生体データ保持部を耐タンパー性のICカードに設けたことで生体データを高い安全性でもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感を低減させることができる。

【0016】次に、請求項3に対応する発明は、生体測定を行うセンサ、暗号化された生体データを受信しこれを復号化する復号部、並びに、センサにより測定された測定情報と復号化された生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたセンサモジュールと、暗号化された生体データを保持するとともに、当該暗号化された生体データを前記センサモジュールに送出する生体データ保持部、並びに、照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のICカードと、センサモジュールとICカードとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0017】本発明はこのような手段を設けたので、請求項2に対応する発明と同様な効果を得ることができる。

【0018】また、請求項4に対応する発明は、請求項3に対応する発明において、センサモジュールに耐タンパー性を持たせた生体データによるユーザ確認システムである。

【0019】本発明はこのような手段を設けたので、請求項3に対応する発明と同様な効果を得ることができる。他、生体データ等の安全性を一層高めることができる。

【0020】さらに、請求項5に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、暗号化された生体データを受信しこれを復号化する復号部、並びに、センサにより測定された測定情報と復号化された生体データとを照合するとともに、照合結果より本人と確認されたときにはその旨の通知を出力する照合計算部を備えたコンピュータと、暗号化された生体データを保持するとともに、当該暗号化された生体データをコンピュータに送出する生体データ保持部、並びに、照合計算部からの通知を受けると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理部を備えた耐タンパー性のICカードと、センサモジュールとICカードとコンピュータとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0021】本発明はこのような手段を設けたので、請求項2に対応する発明と同様な効果はある程度は得られるとともに、簡易にかつ安価なシステムを構築することができる。

【0022】さらにまた、請求項6に対応する発明は、請求項1～5に対応する発明において、ICカードはユーザ本人のデジタル署名を行う署名手段を備え、ユーザ確認がされたことに対応してなされるデータ出力には、署名手段によるデジタル署名が含まれる生体データによるユーザ確認システムである。

【0023】本発明はこのような手段を設けたので、請求項1～5に対応する発明と同様な効果が得られる他、

ICカードを用いたデジタル署名システムを構築することができる。

【0024】一方、請求項7に対応する発明は、生体測定を行うセンサを備えたセンサモジュールと、ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を当該ユーザが有することを示す情報として保持する生体データ保持部、並びに、ユーザ要求及びログオンパスワードが入力されたときに生体データ保持部の生体データをログオンパスワードにより復号化するとともに、この復号化された生体データとセンサにより測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、ユーザ要求を実施すべき旨の通知を出力する照合計算部を備えたコンピュータと、コンピュータとセンサモジュールとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0025】本発明はこのような手段を設けたので、パスワードで暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。また、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、使用上の煩わしさを少なくしユーザ本人確認の確実性を高くすることができる。

【0026】また、請求項8に対応する発明は、生体測定を行うセンサと、コンピュータと、ICカードとからなり、ユーザ確認を行うとともにデータの暗号化処理を行うユーザ確認システムにおいて、ICカードは、耐タンパー性を有し、かつ、生体データを保持する生体データ保持部、データの暗号化処理におけるその一部処理を実行する第1の暗号計算部、並びに、第1の暗号計算部での処理に用いられる暗号鍵を保持する暗号鍵保持部を少なくとも備えており、コンピュータは、ユーザ確認通知を受けるとデータの暗号化処理における他の処理を実行する第2の暗号計算部を少なくとも備えており、さらに、センサにより測定された測定情報と生体データ保持部内の生体データとを照合するとともに、照合結果より本人と確認されたときには第2の暗号計算部にユーザ確認通知を出力する照合計算手段と、センサとICカードとコンピュータとの間の通信を行う通信手段とからなる生体データによるユーザ確認システムである。

【0027】本発明はこのような手段を設けたので、生体データ及び暗号鍵が耐タンパー性の高いICカードに格納され、確実なユーザ本人確認がなされた後に暗号化処理を実行することができる。また、ICカードとコンピュータとで暗号化処理を分担するようにしているので、極めて秘匿性の高い暗号化を実現することができる。

【0028】さらに、請求項9に対応する発明は、コンピュータに、ユーザ本人のログオンパスワードにより暗号化された生体データを、ユーザ要求に対応した権限を

当該ユーザが有することを示す情報として保持する生体データ保持機能と、ユーザ要求及びログオンパスワードが入力されたときに生体データをログオンパスワードにより復号化するとともに、この復号化された生体データと生体測定された測定情報とを照合し、その照合結果により本人及び権限が確認されたときには、ユーザ要求を実施すべき旨の通知を出力する照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0029】本発明はこのような手段を設けたので、請求項7に記載した生体データによるユーザ確認システムにおけるコンピュータの動作を実現させることができる。

【0030】さらにまた、請求項10に対応する発明は、コンピュータに、ユーザ確認通知を受けた場合には、データの暗号化処理における一部処理を実行するとともに、このデータ暗号化処理における他の処理の処理結果を外部から受け取り、その処理結果を用いて暗号化処理を完成させる暗号計算機能と、生体測定された測定情報とユーザ確認用の生体データとを照合するとともに、照合結果よりユーザ本人と確認されたときには暗号計算機能にユーザ確認通知を行う照合計算機能とを実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0031】本発明はこのような手段を設けたので、請求項8に記載した生体データによるユーザ確認システムにおけるコンピュータの動作を実現させることができる。

【0032】一方、請求項11に対応する発明は、暗号化された生体データを保持するとともに、この暗号化された生体データを外部装置に出力する生体データ保持手段と、生体データと生体測定された測定情報とによりユーザ本人と確認された旨の照合結果を外部装置から通知されると、ユーザ確認がされたことに対応してなされるデータ出力を実行する演算処理手段とを備え、かつ耐タンパー性を有することを特徴とするICカードである。

【0033】本発明はこのような手段を設けたので、請求項3又は5に記載した生体データによるユーザ確認システムにおけるICカードの動作を実現させることができる。

【0034】次に、請求項12に対応する発明は、請求項11に対応する発明において、外部装置は、生体測定を行うセンサを有するセンサモジュールであるICカードである。

【0035】本発明はこのような手段を設けたので、請求項3又は4に記載した生体データによるユーザ確認システムにおけるICカードの動作を実現させることができる。

【0036】また、請求項13に対応する発明は、請求項11に対応する発明において、外部装置は、コンピュ

10

20

30

40

50

ータであるICカードである。

【0037】本発明はこのような手段を設けたので、請求項5に記載した生体データによるユーザ確認システムにおけるICカードの動作を実現させることができる。

【0038】さらに、請求項14に対応する発明は、請求項11～13に対応する発明において、演算処理手段はユーザ本人のデジタル署名を行う署名手段を備え、ユーザ確認がされたことに対応してなされるデータ出力には、署名手段によるデジタル署名が含まれるICカードである。

【0039】本発明はこのような手段を設けたので、請求項3～5に対応する発明のうち、さらに請求項6の手段も有する生体データによるユーザ確認システムにおけるICカードの動作を実現させることができる。

【0040】また、請求項15に対応する発明は、生体データを保持するとともに、この生体データを用いてユーザ確認を行う外部装置に生体データを出力する生体データ保持手段と、データの暗号化処理における一部処理を暗号鍵を用いて実行するとともに、このデータの暗号化処理における他の処理を行う外部装置に一部処理の処理結果を出力する暗号計算手段と、暗号鍵を保持する暗号鍵保持手段とを備え、かつ耐タンパー性を有するICカードである。

【0041】本発明はこのような手段を設けたので、請求項8に記載した生体データによるユーザ確認システムにおけるICカードの動作を実現させることができる。

【0042】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

【0043】本発明は、すでに述べたように、1) 生体データの漏洩危険性を低減させること、2) 自己の生体データを情報機器を格納することに対するユーザの抵抗感を低減させること、を目的としており、上記1)、2)の何れか若しくは両方を実現できる手段を提供するものである。

【0044】特に、発明者らは、生体データによるユーザ確認システムの一形態としてのICカード署名システムに、バイオメトリクスを適用させる場合にいかなるシステムを構築すれば上記目的を実現できるかについて種々検討した。ここで、ICカード署名システムとは、ICカード内部のデジタル署名機能を作動させる機能をもったICカードを利用し、そのデジタル署名により、機密情報の電子メールによる送付、インターネット上の買い物等を実現させるシステムである。このシステムにバイオメトリクスを適用させた場合には、指紋等の生体データについてのセンサ測定情報との照合結果に基づき本人確認を行い、その上でICカードの上記デジタル署名機能を作動させることになる。

【0045】発明者らは、まず、バイオメトリクスを適用させたICカード署名システム（以下、単にICカー

ド署名システム又はシステムともいう）を構成し得る要素として4つのモジュール、つまりICカード、センサモジュール、コンピュータ（PC、ICカードリーダー/ライター含む）、サーバーについて検討した。次に、ICカード署名システムにおいて行われる処理（生体（登録）データ記録、照合計算）をそれぞれのモジュールで行えば本発明の目的を達成できるかについて検討した。

【0046】図15はバイオメトリクスを適用させたICカード署名システムにおける構成要素及びその組み合わせ結果を示す図である。

【0047】図15に示す各候補システムのうち、生体データがユーザの手元には無い中央処理装置に登録されることを嫌うユーザが存在することを考慮し、ローカルな処理によってICカードの所有者確認を行うことを優先する。そのためサーバーを利用するものは、検討のこの時点では除外した。生体データをユーザ手元の管理範囲に置いて守ることができるシステムであれば、ユーザの抵抗感を低減させることができると考えられるからである。ただし、技術成果の結実である発明を解釈するに当たり、上記ユーザ抵抗感に関し特に問題がない場合には、請求項に記載された範囲内であれば、サーバー等を利用する技術も発明範囲に含まれるものである。

【0048】次に、同一の端末（センサ、PC）を不特定多数で使用可能であること、さらに、同一人物が不特定の端末で使用可能であることの利便性を考慮し、ICカードに生体データを保持するものは候補システムとして残した。

【0049】なお、生体データ保持と照合計算部を一つの耐タンパー性のモジュール内（ICカード又はセンサモジュール）においたものは候補とした残した。この場合、生体データ～照合計算部間の通信が不要となりプロトコルが単純になり、セキュリティも高くできるからである。ここで、耐タンパー性とは、内部の物や情報を原形のまま容易には外部に取り出せないような仕組みを有した性質のことである。この耐タンパー性を実現するには種々の方法が考えられるが、その方法の具体的な例については後述する。

【0050】こうして図15に示すように、多くの組み合わせの中から特に有効と思われる候補システムを5つ見出した。なお、同図中、「PIN」と記したものは、ICカードとPC等との間で機器認証を行うための識別コードであり、署名鍵とは区別している。

【0051】以下、図15に示す候補システムに対応してなされた発明について第1の実施形態から第5の実施形態において説明し、さらに、同図に示さない他のシステムについて第6の実施形態から第8の実施形態において説明する。

【0052】（発明の第1の実施の形態）図1は本発明の第1の実施の形態に係る生体データによるユーザ確認

システムの一例を示す構成図である。

【0053】このユーザ確認システムは、図15の候補システムのうちの耐タンパーモジュール一体型であり、センサモジュール1aと、コンピュータ2aと、ICカード3aとから構成されている。このシステムでは、センサモジュール1a側で生体データ保持と照合計算を行い、ICカード3a側では署名処理のみを行うセンサモジュール1aは、センサ11と、生体データ保持部12と、照合処理部13と、同定文字列格納部14とから構成されている。なお、特に図示しないが、このセンサモジュール1aには、CPU、メモリ等が内蔵され、各種情報処理が実行できるようになっている。

【0054】ここで、センサ11は、生体測定として指紋を測定し電子化情報とする手段であり、生体データ保持部12には各ユーザの生体データが格納されている。また、照合計算部13は、測定されたセンサ情報と生体データを照合し、ユーザ本人か否かを判定するとともに、ユーザ本人であった場合には、その旨の出力を通知する手段である。なお、本実施形態では、照合処理部13は、同定文字列格納部14の同定文字列（以下単にパスワードともいう）をコンピュータ2aを介してICカード3aに出力するようになっている。

【0055】ここで、センサモジュール1aは、スタンドアロン型であり、耐タンパー性を有するものである。なおスタンドアロン型とは耐タンパーセンサモジュール内に少なくともセンサ11と照合計算部13を持つものである。このシステムのセキュリティは、主にセンサモジュール1a内の生体データと照合計算部13の耐タンパー性によっている。このために、センサモジュール1aにおけるセンサ11以外の各部が1チップのICにより構成されている。また、モジュール各構成部分は強固な筐体に格納され、その蓋が開かないようになっている。さらに、強制的に蓋を開けると、生体データ保持部12、照合処理部13及び同定文字列格納部14が格納されるICチップ自体が破壊されるような仕組みになっている。本実施形態ではこの筐体を壁に埋め込んで更なる耐タンパー性を確保している。

【0056】また、センサ11以外の各部12、13、14を1チップのICで構成したこと自体が耐タンパー性を確保することにつながっている。例えばパスワード情報を磁気カードに格納した場合、磁気カードにはその磁気テープ表面に情報がそのまま保持されているので、情報保持の構造さえわかれば容易に上記パスワード情報を読み取ることができ、耐タンパー性が低い。これに対してICチップに情報を格納する場合は、そのチップ端子からコマンド等を電気信号として入力して初めて情報が端子から得られることになる。この操作を実行するのは高い技術が必要であり、その分耐タンパー性が高いと言える。

【0057】また、本実施形態の場合、生体データは同

一のICチップ内でのみ使用されるため、外部出力は不要であり、耐タンパー性を高めるべく生体データの外部出力はできないように構成されている。

【0058】なお、本明細書において、耐タンパー性を有するといった場合には、上記仕組みの何れかあるいはすべてが組み合わされ、また、その他の考え得る措置が取られているものである。また、ここでは、センサモジュールの場合で説明したが、ICカード等の場合でも同様な措置により耐タンパー性を高めることができる。特に、ICカードの場合は、例えばその筐体を開くと鉄粉が配線上に飛び散り、保持情報をすべて消失させるような仕組みを設けることも可能である。

【0059】また、最低限の議論として、単に耐タンパー性があるかないかを考えるときには、例えば保護したい内容が1つのICチップ内に納められているような場合には耐タンパー性はあると言えるであろう。

【0060】次に、コンピュータ2aには、コマンド出力部15と、メッセージ出力部16とが設けられている。また、コンピュータ2aにはICカードリーダ&ライタが含まれ、この点は以下の各実施形態でも同様である。

【0061】さらにコンピュータ2aは特に図示しないが、ブラウザ等の種々のアプリケーションプログラムを実行することが可能であり、本実施形態ではインターネット4に接続されている。

【0062】インターネット4では更にバーチャルモールに接続されており、コンピュータ2aからオンラインショッピングができるようになっている。コンピュータ2aに示される符号「C」は演算（デジタル署名処理等）されたメッセージであるが、後述する本実施形態の動作例ではバーチャルモールに対する物品購入等の要求出力を示している。

【0063】ICカード3aは、確認処理部17と、同定文字列格納部18と、演算処理部19と、秘密鍵保持部20とを備えており、これら各部を実現するCPUやメモリ等の資源が1チップのICに納められたものである。

【0064】確認処理部17は、センサモジュール1aからの同定文字列をICカード内の同定文字列格納部18に格納された同定文字列（パスワード）と比較し、その確認結果を演算処理部19に通知する。つまり、センサモジュール1aとICカード3aは、本人が確認されたか否かの情報をセンサモジュールからICカードへ秘密裏に伝えるための同定文字列を共有していることになる。具体的には、ICカード側の同定文字列はセンサモジュール側の同定文字列と同一であるか、或いは、ちょうどUNIXにおける暗号化パスワードのように、センサモジュール側の同定文字列を暗号化したものでもよい。要するにセンサモジュールから送られた同定文字列に対応して唯一のICカード内同定文字列が対応するよ



うになっている。

【0065】演算処理部19は、システム使用者がユーザ本人であることの確認通知を確認処理部17から受けると、所定の演算処理を実行して、演算されたメッセージCを出力する。このメッセージは、例えば入室管理上の扉開メッセージでもよいし、また例えば計算機等の装置起動命令でもよい。ここで演算処理部19は具体的な一例として、秘密鍵保持部20に格納される秘密鍵を用いてデジタル署名を行うとともに、メッセージ出力部16の情報元をインターネット上のバーチャルモールに物品購入要求を演算されたメッセージCとして出力する。

【0066】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0067】上記したように生体データによるユーザ確認システムは種々の場合に適用できるが、ここでは、インターネット上のバーチャルモールに物品購入要求を出力する場合を例にとってその動作例を説明する。

【0068】図2は本実施形態の動作例を示す流れ図である。

【0069】この動作例では、自宅や会社でコンピュータ2aとしてのパーソナルコンピュータ（パソコン）を立ち上げブラウザソフトを起動し、インターネット4さらにはバーチャルモールに接続して物品購入をしようとする場合を想定している。

【0070】ユーザは、バーチャルモールにおいて商品及びその購入数量を選択決定し、パソコン上の購入ボタンをクリックする。この操作により図1に示すようにコンピュータ2aからコマンド15がセンサモジュール1a及びICカード3aに出力され、各種指示等の表示がコンピュータ2a上になされる（ST1）。

【0071】ここで、ICカード3aがシステムに未挿入の場合には、コンピュータ2aから「ICカードを挿入してください」とのメッセージが出され、ユーザによりICカード3aが挿入される（ST2）。なお、カード挿入に伴いコンピュータ2aから当該カード3aに物品購入処理が開始されたことが通知（コマンド15）される。

【0072】次に、ユーザが自分の指をセンサモジュール1aのセンサ11に押し当てると、センサ11による生体測定が実行される（ST3）。

【0073】次に、測定されたセンサ情報はセンサモジュール1aの照合計算部13において生体データと照合され（ST4）、本人が確認されれば（ST5）、同定文字列格納部14内の同定文字列（パスワード）がICカード3aに出力される（ST6）。なお、この処理は、従来システムにおけるパスワードのキー入力に代わるものである。また、センサモジュール1aからICカード3aへの同定文字列送出において、ハッカーによる

同定文字列の盗聴の危険性を排除するためには、同定文字列を生で送る代わりに暗号化すればよい。

【0074】また、ステップST5において、本人が確認できない場合には、システム使用者がユーザ本人でない旨が表示され、以降の処理は中止される。

【0075】ICカード3aの確認処理部17においては、受信した同定文字列がカード内の保持された同定文字列と比較され、システム使用者がユーザ本人であることが確認される（ST7）。本人確認がなされればその旨が演算処理部19に通知される。

【0076】本人確認の通知を受けた演算処理部19により、メッセージ出力部16からの物品購入情報に基づいてメッセージCが作成されるとともに、そのメッセージCには秘密鍵保持部20に保持される秘密鍵によりデジタル署名が行われる（ST8）。

【0077】こうして作成された演算されたメッセージCは、コンピュータ2aからインターネット4に出力され、バーチャルモールでの物品購入が実現されることになる。

【0078】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、生体データ保持部12と生体データによる照合を行う照合計算部13とを同一のセンサモジュール1a内に格納して生体データがセンサモジュール1a外に出力しないようにし、かつ、センサモジュール1a自体に高い耐タンパー性を持たせたので、生体データの漏洩危険性をほとんど無くすることができ、ひいてはこれによって自己の生体データを情報機器を格納することに対するユーザの抵抗感を低減させることができる。

【0079】また、デジタル署名等を行うに際してパスワード入力でなく、本人への生体測定に基づきユーザ確認をするようにしているので、極めて確実性の高い本人確認を行うことができる。したがって、例えばICカードが紛失したり、盗まれた場合でも第3者による悪用を防止することができる。

【0080】さらに、本システムでは、照合計算部13による照合ののち、その結果をパスワードを用いて演算処理部19に通知するようにしたので、本人を確認してからデジタル署名するまでの処理を安全に行うことができ、極めてセキュリティの高いICカード署名システムを実現することができる。したがって、例えばICカードを含めたシステム全体が盗まれるようなことがあっても、盗難者は生体データを得ることも偽のメッセージCを出力することもできない。なお、このような場合に、秘密鍵や同定文字列が漏洩しないようにICカード3a自体にも高い耐タンパー性が与えられている。

【0081】また、本実施形態のシステムではバイオメトリクスを利用しているので、パスワード等を記憶しておく必要もなく、パスワード入力の煩わしさやその忘却、漏洩の危険性のないシステムを提供することができ

10

20

30

40

50

る。

【0082】さらに、本実施形態では、センサ11、生体データ保持部12、照合処理部13、同定文字列格納部14、確認処理部17、同定文字列格納部18、演算処理部19及び秘密鍵保持部20の各構成要件を図1に示すようにセンサモジュール1a及びICカード3aに配置したので、上記各効果の他、ICカード利用上のメモリも得られる。つまり、従来の署名用のICカードをほとんどそのまま利用することができる。その意味で、本実施形態は既カード利用型とも言える。指紋照合処理の採用を念頭に入れた特殊なICカードを発行する必要がないため、ソフトウェアの変更だけでシステムを導入できる。照合計算部13がICカード3a上にないためICカードへの負荷を小さくできる。

【0083】なお、上記動作例ではバーチャルモールでの買い物の場合で説明したが、より具体的には、例えばSET (Secure Electronic Transaction)の購入要求への導入が考えられる。SETは元来磁気カードを念頭に置いた仕様であるが、実用形態としてはICカード(＋パスワード)の使用もできる。カード会員による検証と購入要求における「会員の秘密鍵で署名」の処理に本実施形態で説明した技術を導入するとその有用性が高まると考えられる。

【0084】また、本実施形態では、生体データとして指紋を用いたが、本発明はこれに限られるものでなく、掌型や声紋、網膜、顔写真等、その他種々の生体データを用いる場合にも適用することができる。また、センサ11とICカード内のデジタル署名機能部分19、20とが分離しているので、使用するセンサ種類の自由度を大きくすることができる。

【0085】さらに、本実施形態のシステムでは、センサモジュール1aの生体データ保持部12に複数の生体データをできるようにすることで、個人用のシステムとしてだけでなく、複数人が同一システムを使用できるようにすることも可能である。

(発明の第2の実施の形態)図3は本発明の第2の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0086】このユーザ確認システムは、図15の候補システムのうちの万能ICカード型であり、センサモジュール1bと、コンピュータ2bと、ICカード3bとから構成されている。本システムでは、センサモジュール1bではセンサ入力情報送信のみ(簡単なスクランブル処理は行い、ICカード3b側で署名処理に加えて生体データ保持と照合計算を行う。

【0087】図3に示す各構成におけるセンサ11、生体データ保持部12、照合処理部13、確認処理部17、演算処理部19及び秘密鍵保持部20の機能は第1

の実施形態の図1に示されるものと同様である。ただし、その各部の配置場所が異なっている。

【0088】すなわち、本実施形態では、センサモジュール1bにはセンサ11のみが設けられている。一方、ICカード1bには、生体データ保持部12、照合処理部13、確認処理部17、演算処理部19及び秘密鍵保持部20が設けられ、これらは同一ICチップ内に構成される。なお、コンピュータ2bの構成は第1実施形態のコンピュータ2aと同様である。

【0089】各部がこのような配置されることからセンサモジュール1bにはそれほど高い耐タンパー性は必要ないが、ICカード3bには高い耐タンパー性が要求され、第1の実施形態で説明したような手段で耐タンパー性が確保されている。

【0090】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0091】ここでも第1の実施形態と同様にインターネット4上のバーチャルモールへのアクセスを例にとって説明する。

【0092】図4は本実施形態の動作例を示す流れ図である。

【0093】同図において、ステップST11からST13までの処理は第1の実施形態の図2ステップST1からST3までと同様である。

【0094】次に、センサモジュール1bからは測定されたセンサ情報がICカード3bに送出される(ST14)。センサ情報を受け取ったICカード3bでは第1の実施形態のセンサモジュール1a内で処理と同様な照合が実行される(ST15)。なお、この照合処理はICカード3b内のみで行われるので、耐タンパー性を高めるため、生体データ保持部12の生体データはICカード3bから外部に出力できない構成となっている。

【0095】照合により本人確認がなされると(ST16)、その確認結果が演算処理部19に通知され(ST17)、以下第1実施形態と同様に、デジタル署名等行われ(ST18)、演算されたメッセージCがバーチャルモールへ出力される(ST19)。

【0096】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、照合処理部13と生体データ保持部12を同一のICカード3bに格納するとともに、当該カード3bの耐タンパー性を高めたので、生体データの漏洩危険性を低減させることができるとともに、生体データを高い安全性でもってユーザ手元の管理範囲(ICカード)に置いて守ることができ、自己の生体データを情報機器を格納することに対するユーザの抵抗感を大幅に低減させることができる。つまり、個人所有するICカードにセンサ以外の主要な要素がすべて実装されているため、心理的にも安心感が強い。

10

20

30

40

50

【0097】また、照合計算部13と演算処理部19が同一ICチップ内に構成されるので、本人を確認してからデジタル署名するまでの処理を安全に行うことができ、極めてセキュリティの高いICカード署名システムを実現することができる。

【0098】また、本実施形態のシステムでは、センサモジュール側では比較的原始的な信号処理のみを受け持たせているので、センサモジュール1bの負担を小さくすることができる。

【0099】万能ICカード型は照合装置に対して特別な要請は無く、どの型の指紋照合装置でも適用可能である。このシステムのセキュリティはもっぱらICカードの耐タンパー性に基づいており、暗号通信を用いた工夫は行っていないためシンプルな構造となっている。ICカード3bに多くの機能(生体データ保持、照合計算部、署名処理、署名鍵保持、)を持たせたため、ICカード3bへの負荷は大きい。したがって、この用途に限定した専用のICカードを発行するとより効果的なシステム運用が可能となる。

【0100】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【0101】(発明の第3の実施の形態)図5は本発明の第3の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0102】このユーザ確認システムは、図15の候補システムのうちのICカードにデータ～センサ計算型であり、センサモジュール1cと、コンピュータ2cと、ICカード3cとから構成されている。本システムでは、センサモジュール側で照合計算を行い、ICカード側に生体データを保持する。

【0103】センサモジュール1cは、スタンドアロン型であり、センサ11と、照合計算部13と、同定文字列保持部14と、復号処理部21と、復号鍵保持部22とから構成されている。

【0104】また、ICカード3cは、確認処理部17と、同定文字列保持部18と、演算処理部19と、秘密鍵保持部20と、暗号化生体データ保持部12bとから構成されている。ここで、センサモジュール1c及びICカード3cは耐タンパー性の高い構成となっている。

【0105】ICカード3cにおける暗号化生体データ保持部12bには、ICカード保持者の生体データが復号鍵保持部22に格納される復号鍵で復号できるように暗号化され保持されている。

【0106】また、センサモジュール1cの復号処理部21は、ICカード3cから受け取った暗号化生体デー

タを復号鍵保持部22に格納される復号鍵で復号して照合計算部13に提供しようとしている。

【0107】なお、コンピュータ2cは、第1の実施形態と同様に構成される。

【0108】このように構成された本発明の実施の形態に係る生体データによるユーザ確認システムは次に説明するように動作する。

【0109】ここでも第1の実施形態と同様にインターネット4上のバーチャルモールへのアクセスを例にとって説明する。

【0110】図6は本実施形態の動作例を示す流れ図である。

【0111】同図に示す本実施形態の生体データによるユーザ確認システムにおいて、コマンド出力(ST21)及びICカード挿入(ST22)、並びに、センサによる生体測定が行われ(ST25)、センサモジュールにおけるセンサ情報と生体データの照合された以降の処理(ST26～ST31)は、図2に示す第1の実施形態の場合(図2:ST1～ST2並びにST3～ST9)と同様である。したがって、この部分の処理は説明を省略する。

【0112】本実施形態の特徴は、ICカード3cに保持された暗号化生体データがICカード3cからセンサモジュール1cに送出されるとともに(ST23)、その生体データがセンサモジュール1c内の復号処理部21及び復号鍵保持部22の復号鍵により復号され(ST24)、ステップST26の照合計算に提供されるところにある。

【0113】本人確認並びにデジタル署名等の処理体系をこのような構成動作としたことによる効果について以下に説明する。

【0114】本発明の実施の形態に係る生体データによるユーザ確認システムは、個人が所有する演算(例えばデジタル署名)機能付きICカード3cに本人の生体データを保持し、暗号化された生体データを特定の場所に常置されたセンサモジュール1cに送って当該センサモジュール1cにて照合計算を行うようにし、さらにセンサモジュール1c及びICカード3cに高い耐タンパー性を持たせたので、生体データが漏洩したりICカードが他人に不正に使用されたりすることなく、安全に演算(例えばデジタル署名)を行うことができる。

【0115】また、生体データは暗号化されてICカード3cのみに格納されているので、生体データの漏洩危険性を低減させることができるとともに、生体データを高い安全性をもってユーザ手元の管理範囲(ICカード)に置いて守ることができ、自己の生体データを情報機器を格納することに対するユーザの抵抗感を大幅に低減させることができる。

【0116】さらに、本実施形態のシステムは、多くのバイOMETRICSセンサ(掌型、網膜など)はその大き

さや仕組みからICカード上に実装できないことや、照合計算をICカードの中で行うには比較的負荷が大きいことを考え合わせると、様々な組み合わせの中でも作り易くバランスの良いシステムとなっている。

【0117】しかしながら、照合を行う度に毎回ICカードから個人の生体データをセンサモジュールの照合計算部13へ送る必要があるため、セキュリティ保持のために上記した暗号化処理が行われている。図5は、なるべく簡素でありながら十分なセキュリティを保つことのできる例として、センサ側に保持された復号鍵によって暗号化された生体データをICカードに保持するシステムとなっている。ICカード3cに生体データがあり、高いセキュリティが保持される。

【0118】したがって、本実施形態のシステムは、不特定多数で簡単に利用可能、つまり本システムに対応した多くの場所(システム)で使用可能であり利便性が高い。すなわち、ICカードに個人の生体データを持つため、一つのシステムを不特定多数で使う場合に適している。ただし、ICカードに生体データを格納する必要があるため、署名用に作られたICカードにさらに生体データ専用のメモリが追加されている。

【0119】構造的にはこのメモリと署名処理の部分は切り分けられるため、第2の実施形態で示した万能ICカード型の場合に比べればICカードの設計変更は容易である。また、照合計算をセンサモジュール1cで行うのでICカード3cの負荷も小さく、現実的なシステムとすることができる。なお、ハッカーによる同定文字列の盗聴の危険性を排除するためには同定文字列を暗号化してICカードに送るのが好ましいことは第1の実施形態と同様である。

【0120】また、暗号化生体データは毎回そのまま同じものをICカード3cからセンサモジュール1c側に送っているが、登録データと全く同一のセンサ情報は受け付けないという簡単な仕組みを照合計算部13内に設けると、より高いセキュリティが保たれる。というのは通常バイオメトリクスセンサからの情報には誤差があり、登録されているデータと全く同一のデータが取得されることは殆ど有り得ないからである。全く同一のデータを拒否することにより正規ユーザの使用を妨げること無く、不正なコピーなどによって登録データ(生体データ)を入手した侵入者の使用を排除できるという効果が期待される。

【0121】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【0122】(発明の第4の実施の形態)図7は本発明の第4の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分に

は同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0123】このユーザ確認システムは、図15の候補システムのうちのICカードにデータ~PC計算型であり、センサモジュール1dと、コンピュータ2dと、ICカード3dとから構成されている。このシステムでは、センサモジュール側ではセンサ入力情報送信のみ(簡単なスクランブル処理は行う)を行い、ICカード1dに生体データを保持し、コンピュータ(PC)で照合計算を行う。

【0124】本実施形態のユーザ確認システムでは、ICカード3d自体は、第3の実施形態のICカード3cと同様に構成され、センサモジュール1dは、第2の実施形態のセンサモジュール1bと同様に構成されている。

【0125】また、コンピュータ2dには、第1の実施形態と同様な構成に加え、第3の実施形態のセンサモジュール1cにおけるセンサ11以外の構成部分が照合機能部23として設けられている。なお、この照合機能部23は、照合計算部13と、同定文字列保持部14と、復号処理部21と、復号鍵保持部22とからなっており、DLL(ダイナミックリンクライブラリ)として構成させることも可能である。なお、DLLは、コマンドがスタートしたときに初めて呼ばれるプログラムである。

【0126】このように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0127】図8は本実施形態の動作例を示す流れ図である。

【0128】同図に示すように、本実施形態のユーザ確認システムは、ステップST43~ST48の処理がセンサモジュール1dでなくコンピュータ2dにより若しくはコンピュータ2dに対して行われる点を除けば、図6に示す第3の実施形態のシステムと同様に動作する。

【0129】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、コンピュータ2dの内部に照合機能部23を設けるようにしたので、ある程度の生体データの漏洩危険性の低減、並びに、確実性の高い本人確認機能、すなわちICカードが紛失したり、盗まれた場合でも第3者による悪用の防止を可能としつつ、これらの機能を簡単なハードウェアで実現し経済的かつ現実性の高いシステムとすることができる。

【0130】なお、本実施形態と上記各実施形態との関係で共通した構成に対応した効果は、本実施形態においても当然にして得られるものであり、上記何れかの実施形態で説明した効果についてはここでは説明を省略する。

【0131】(発明の第5の実施の形態)図9は本発明

10

20

30

40

50

の第5の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0132】このユーザ確認システムは、図15の候補システムのうちのICカード一体型であり、コンピュータ2eと、ICカード3eとから構成されている。

【0133】本実施形態のICカード3eには、センサ11、生体データ保持部12、照合処理部13、演算処理部19及び秘密鍵保持部20が設けられており、これらの各構成がセンサ11も含めてICの1チップ内に納められている。また、生体データは耐タンパー性を高めるために外部に出力できないように構成されており、ICカード3eには、耐タンパー性を高めるための上記各仕組みが設けられている。

【0134】なお、コンピュータ2eは、アクセス対象がICカード3eのみであることを除けば第1の実施形態と同様に構成されている。

【0135】このように構成された生体データによるユーザ確認システムの動作は、センサ11自体がICカード2e内に設けられ、ICカード2eにて生体測定が行われセンサ情報の機器間移動がない点を除けば、第2の実施形態と同様である。

【0136】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、第2の実施形態の構成を有するICカードにさらにセンサ11を設けて秘匿性の高い情報は全てICカード3eの内部で処理するようにしたので、第2の実施形態とその構成が共通する部分について同様な効果が得られる他、暗号通信を用いた工夫は不要でありシンプルでプロトコル構造とすることができる。また、耐タンパー性自体も高いものとすることができる。

【0137】（発明の第6の実施の形態）本実施形態は、計算機ソフトウェアの使用権限を、生体データを利用したバイオメトリクスによる個人認証で確認するシステムである。本システムは、ICカード等の耐タンパー性の携帯物を使用することなく、また、生体データが漏洩したり他人に不正に使用されたりすることなく、ソフトウェアの使用許可を安全に行うものである。

【0138】図10は本発明の第6の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0139】このユーザ確認システムは、センサモジュール1fとコンピュータ2fとから構成されている。

【0140】センサモジュール1fは、第2実施形態と同様に構成されており、センサ11を備えたものである。

【0141】コンピュータ2fには、照合計算部31aと、暗号化生体データ保持部32aと、スクリーンセー

バー等の起動対象ソフトウェア34aが設けられている。

【0142】暗号化生体データ保持部32aには、各ユーザのログオンパスワードで予め暗号化された各ユーザの生体データが保持されている。

【0143】照合計算部31aは、生体データとセンサ測定情報により個人認証を行い、使用権限者と確認できれば対象ソフトウェア34aに起動命令を出力する。

【0144】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0145】まず、対象ソフトウェア34aを使い始める際に、ユーザにより入力装置（図示せず）を介してログオンパスワード33aが入力される。

【0146】次に照合計算部31aにより、対象ソフトウェア34aの使用権限を有する暗号化生体データが生体データ保持部32aから読み出され、入力ログオンパスワード33aによる復号化が行われる。

【0147】次に、センサモジュール1fにおいて生体測定が行われ、その測定結果がコンピュータ2fの照合計算部31aに送信される。なお、この送信データには簡単なスクランブルがかけられている。

【0148】照合計算部31aでは、復号化された生体データと、受信したセンサ情報を照合し、システムを使用している者が起動対象のソフトウェア34aの使用権限を有するか否かを確認する。なお、ログオンパスワード33a、復号化された生体データ及び受信したセンサ情報は揮発性メモリ上のみ記録され、セッション終了後はこれらの情報は消えるようになっている。

【0149】上記照合計算により、ソフトウェア起動の要求をしている者が正当な使用権限を有するユーザ本人であると確認されると、照合計算部31aによりその旨が起動対象ソフトウェア34aに通知される。これにより、起動対象ソフトウェアの起動処理が開始される。

【0150】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、ログオンパスワード33aを入力することにより、当該ログオンパスワードで暗号化された生体データが復号され、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、パスワードで暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。

【0151】さらに、パスワード等は揮発性メモリ上のみ記録され、セッションを終了すると情報は消え去るため、何らかの手段でハードディスク等に記録された不揮発性の情報を読まれることがあってもパスワード情報等が盗まれることはない。

【0152】なお、本実施形態では、ソフトウェア使用権限の場合で説明したが、本発明はソフトウェア起動の

場合に限られるものでなく、例えば計算機自体の起動や各種機器の起動についても本実施形態の技術を適用させることができる。

【0153】また、例えば本実施形態の技術を用いてユーザ確認及び権限確認をしつつ計算機の起動をした場合に、そのユーザが使用権限を有するソフトウェアのリストを表示し、以降、リスとアップされたソフトウェアの使用は自由にできるようにしてもよい。このようにすれば、ソフトウェア起動時に一々生体測定をする必要がなく、ユーザの負担を軽減することができる。

【0154】（発明の第7の実施の形態）図11は本発明の第7の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0155】このユーザ確認システムは、センサモジュール1gとコンピュータ2gとICカード3gとから構成されている。

【0156】センサモジュール1gは、第2実施形態と同様に構成されており、センサ11を備えたものである。

【0157】コンピュータ2gには、照合計算部31bと、起動対象ソフトウェア34bとが設けられている。

【0158】ICカード3gには、暗号化された生体データを保持する暗号化生体データ保持部32bと、この暗号化生体データを復号するための暗号鍵を保持する暗号鍵保持部35と、ログオンパスワードを保持するログオンパスワード保持部36とが設けられている。なお、ICカード3gは高い耐タンパー性を有するものである。

【0159】コンピュータ2gの照合計算部31bは、生体データ及びセンサ11の生体測定結果からユーザ本人を確認し、その結果を起動対象ソフトウェア34bに通知する。

【0160】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0161】まず、ICカード3gが挿入されると、起動対象ソフトウェア34bによりICカード内のログオンパスワードが読み取られ、照合計算部31に本人確認の依頼がなされる。

【0162】起動対象ソフトウェア34bに依頼された照合計算部31bによって、生体測定情報がセンサ11に要求されるとともに、ICカード3gの暗号化生体データ保持部32b及び暗号鍵保持部35から暗号化生体データ及びその暗号鍵が読み出される。

【0163】これらの情報を受け取った照合計算部31bは暗号化生体データを復号して生体データを取り出すとともに、センサ11から生体測定情報を受け取り、両者を比較照合してユーザ本人か否か確認する。

【0164】本人であることが確認されればその旨が起動対象ソフトウェア34bに通知され、起動対象ソフトウェア34bの起動が開始される。

【0165】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、ICカード3gをコンピュータ2gに挿入するだけで、暗号鍵で暗号化された生体データが復号され、バイオメトリクスを用いたユーザ本人確認及び権限確認がなされるようになっているので、暗号鍵で暗号化された生体データはたとえ単独で漏洩してもその秘密を守ることができ、かつソフトウェアの使用権限をも守ることができる。

【0166】さらに、コンピュータにおいて生体データ等は揮発性メモリ上のみ記録され、セッションを終了すると情報は消え去るため、これらの情報が盗まれることはない。

【0167】なお、本実施形態では、ソフトウェア使用権限の場合で説明したが、本発明はソフトウェア起動の場合に限られるものでなく、例えば計算機自体の起動や各種機器の起動についても本実施形態の技術を適用させることができる。

【0168】また、例えば本実施形態の技術を用いてユーザ確認及び権限確認をしつつ計算機の起動をした場合に、そのユーザが使用権限を有するソフトウェアのリストを表示し、以降、リスとアップされたソフトウェアの使用は自由にできるようにしてもよい。このようにすれば、ソフトウェア起動時に一々生体測定をする必要がなく、ユーザの負担を軽減することができる。

【0169】（発明の第8の実施の形態）本実施形態は、ファイル暗号化用の暗号鍵を記録したICカードに生体データも記録することにより、暗号処理のセキュリティを高めたファイル暗号化システムとしてのユーザ確認システムを提供するものである。

【0170】図12は本発明の第8の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図であり、図1と同一部分には同一符号を付して説明を省略し、ここでは異なる部分についてのみ述べる。

【0171】このユーザ確認システムは、センサモジュール1hとコンピュータ2hとICカード3hと二次記憶装置としてのハードディスク5とから構成されている。

【0172】センサモジュール1hは、第2実施形態と同様に構成されており、センサ11を備えたものである。コンピュータ2hには、照合計算部31cと、暗号化プログラム37が設けられている。また、ICカード3hには、生体データ保持部32cと、暗号計算部38と、暗号鍵保持部39とが設けられている。さらに、ハードディスク5には、暗号若しくは復号対象となる入力ファイル40と、暗号若しくは復号結果としての出力ファイル41とが設けられている。

【0173】照合計算部31cは、生体データとセンサ

情報とからユーザ本人を確認し、暗号化プログラム37並びに暗号計算部38にファイル暗号化開始許可の通知をするようになっている。

【0174】暗号化プログラム37は、入力ファイル40を読み込み、その暗号若しくは復号対象情報を暗号計算部38と協力して暗号若しくは復号し、その結果を出力ファイル41に出力する。

【0175】暗号計算部38は、暗号化プログラム37が行う暗号若しくは復号処理の一部を担っており、自身が行うその暗号若しくは復号処理部分において暗号鍵保持部39の暗号鍵を使用する。

【0176】なお、ICカード3hは高い耐タンパー性を有するものである。

【0177】次に、以上のように構成された本発明の実施の形態に係る生体データによるユーザ確認システムの動作について説明する。

【0178】図13は本実施形態の全体動作を示す流れ図である。

【0179】まず、暗号化プログラム37の起動を開始する(ST61)。暗号化プログラム37は照合計算部31cにシステム使用者が本人であるか否かの確認を依頼する。

【0180】次に挿入されたICカード3hから生体データが照合計算部31cに読み取られる(ST62)。なお、特に図示しないが生体データ保持部32cに格納され送出される生体データは、本実施形態の方法あるいは第3の実施形態の方法等で暗号化されたものであり、照合計算部31cにおいて復号化されて用いられる。

【0181】次に、センサ11による生体測定が行われ、センサ情報が照合計算部31cに送出される(ST63)。なお、この送信データには簡単なスクランブルがかけられている。

【0182】次に、照合計算部31cにて生体データとセンサ情報の照合が行われ、システム使用者がユーザ本人であるか否かの確認がなされる(ST64)。なお、復号化された生体データ及び受信したセンサ情報は揮発性メモリ上のみ記録され、セッション終了後はこれらの情報は消えるようになっている。

【0183】上記照合をした結果、本人でなければエラー表示して終了し、本人と確認されれば、その旨の通知が暗号化プログラム37及び暗号計算部38になされる(ST65)。

【0184】これによって、暗号化プログラム37及び暗号計算部38の起動が終了し、ファイルの暗号化処理が開始される(ST66)。

【0185】すなわち入力ファイル40が暗号化プログラム37に読み込まれ(ST67)、暗号化若しくは復号化処理が実行されて(ST68)、その結果が出力ファイルに出力され(ST69)、一連の処理が終了する。

【0186】次に、ステップST68における暗号化処理について詳しく説明する。

【0187】図14は本実施形態における暗号化処理を示す流れ図である。

【0188】まず、暗号化プログラム37において、暗号化の鍵として乱数が発生され(ST71)、当該乱数を鍵として読み込まれた暗号化対象データ(平文)が暗号化される(ST72)。

【0189】この乱数はICカード3h内の暗号計算部38に送出され(ST73)、この暗号計算部38において暗号鍵保持部39内の暗号鍵により暗号化される(ST74)。

【0190】暗号化した乱数は暗号計算部38によってコンピュータ2hの暗号化プログラム37に送出される(ST75)。

【0191】受信された暗号化乱数は、暗号化プログラム37によってステップST72で平文を暗号化した暗号文のヘッダとして付加され、全体として一つの暗号文が構成される(ST76)。すなわち、ステップST72で暗号化されたものを暗号文本体とし、ステップST75で暗号化された乱数をヘッダとして暗号文を生成する。

【0192】こうして生成された暗号文がハードディスク5に出力されることになる。

【0193】一方、図13のステップST68における復号化処理は上記暗号化処理の逆の処理が行われることになる。

【0194】すなわちまず、暗号化プログラム37は、復号対象の暗号文におけるヘッダのみを暗号計算部38に送り、暗号計算部38ではそのヘッダを暗号鍵保持部39内の鍵で復号する。

【0195】こうして復号された情報は、復号対象の暗号文の本文を暗号化するのに用いた鍵としての乱数である。

【0196】この取り出された乱数が暗号計算部38から暗号化プログラム37に送出される。この乱数を受信した暗号化プログラム37は、受信乱数により暗号文本文を復号し、もとの平文を取り出す。

【0197】こうして復号された平文がハードディスク5に出力されることになる。

【0198】上述したように、本発明の実施の形態に係る生体データによるユーザ確認システムは、生体データ及び乱数用の暗号鍵を耐タンパー性の高いICカード3hに格納するようにしたので、極めて秘匿性の高い暗号化処理を確実にユーザ本人確認してから実行することができる。

【0199】また、本実施形態では乱数を用いた間接的な暗号化処理を行うようにしたので、暗号化処理と復号処理を行うたびに異なる乱数が使われ、万一1個の乱数が解読されても、次の暗号化処理と復号処理の秘密は

守られ、確実なユーザ確認と高セキュリティと兼ね備えた暗号化システムを実現することができる。

【0200】さらに、上記暗号復号処理に使用される ICカード 3h 内の暗号鍵は ICカード内の暗号計算部 38 でのみ使われ、ICカード 3h の外部には出ることなく、かつ、この暗号鍵は耐タンパー性の高い ICカード 3h 内に格納されているので、暗号の秘匿性をより高めることができる。

【0201】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に 10 変形することが可能である。

【0202】また、実施形態に記載した手法は、計算機（コンピュータ）に実行させることができるプログラム（ソフトウェア手段）として、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（CD-ROM、DVD等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。なお、媒体側に格納されるプログラムには、計算機に実行させるソフトウェア手段（実行プログラムのみならずテーブルやデータ構造も含む）を計算機内に 20 構成させる設定プログラムをも含むものである。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、また場合により設定プログラムによりソフトウェア手段を構築し、このソフトウェア手段によって動作が制御されることにより上述した処理を実行する。

【0203】

【発明の効果】以上詳記したように本発明によれば、生体データを高い安全性をもってユーザ手元の管理範囲に置いて守ることができ、ひいてはユーザの抵抗感及び生体データの漏洩危険性を低減することを可能とし、さら 30 に使用上の煩わしさが少なくユーザ確認の確実性が高い生体データによるユーザ確認システム及び ICカード並びに記録媒体を提供することができる。

【図面の簡単な説明】

【図 1】本発明の第 1 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 2】同実施形態の動作例を示す流れ図。

【図 3】本発明の第 2 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 4】同実施形態の動作例を示す流れ図。

【図 5】本発明の第 3 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 6】実施形態の動作例を示す流れ図。

【図 7】本発明の第 4 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 8】同実施形態の動作例を示す流れ図。

【図 9】本発明の第 5 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 10】本発明の第 6 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 11】本発明の第 7 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 12】本発明の第 8 の実施の形態に係る生体データによるユーザ確認システムの一例を示す構成図。

【図 13】同実施形態の全体動作を示す流れ図。

【図 14】同実施形態における暗号化処理を示す流れ図。

【図 15】バイオメトリクスを適用させた ICカード署名システムにおける構成要素及びその組み合わせ結果を示す図。

【符号の説明】

1a, 1b, 1c, 1d, 1f, 1g, 1h…センサモジュール

2a, 2b, 2c, 2d, 2e, 2f, 2g, 2h…コンピュータ

3a, 3b, 3c, 3d, 3e, 3g, 3h…ICカード

4…インターネット等

5…ハードディスク

11…センサ

12…生体データ保持部

13…照合処理部

14…同定文字列格納部

15…コマンド出力部

16…メッセージ出力部

17…確認処理部

18…同定文字列格納部

19…演算処理部

20…秘密鍵保持部

21…復号処理部

22…復号鍵保持部

23…照合機能部

31a…照合計算部

32a…暗号化生体データ保持部

34…起動対象ソフトウェア

37…暗号化プログラム

38…暗号計算部

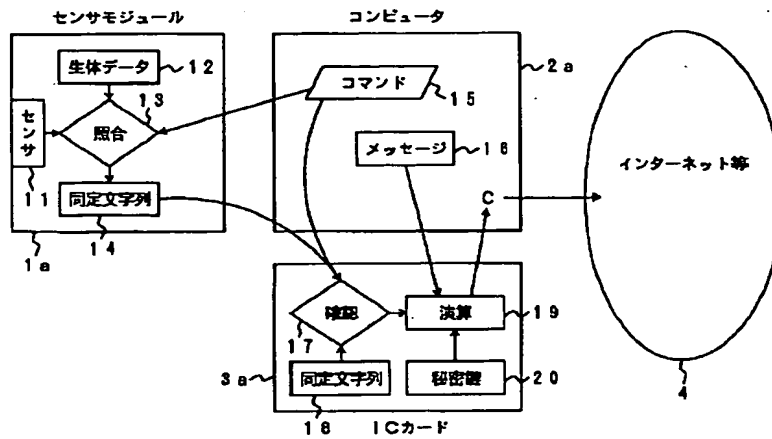
39…暗号鍵保持部

40…入力ファイル

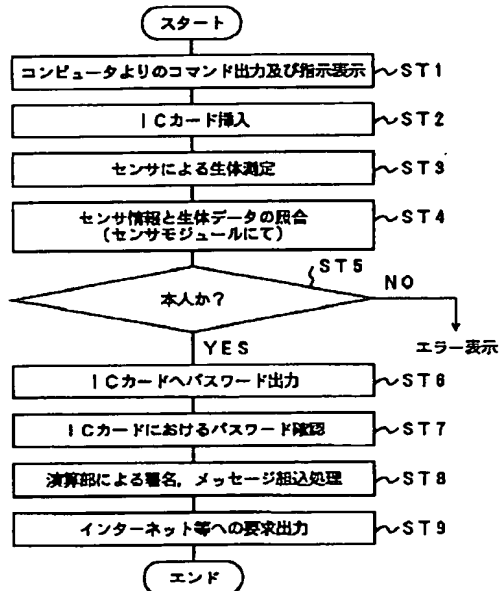
41…出力ファイル



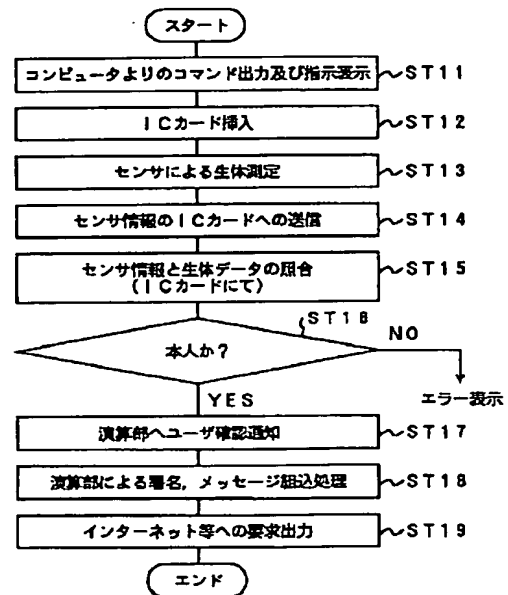
【図1】



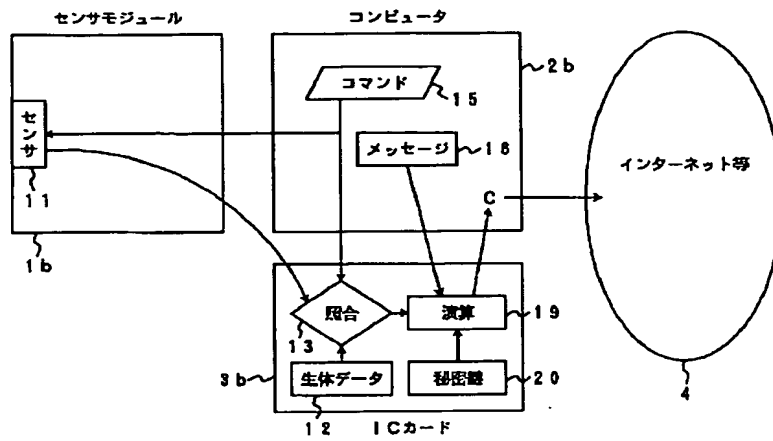
【図2】



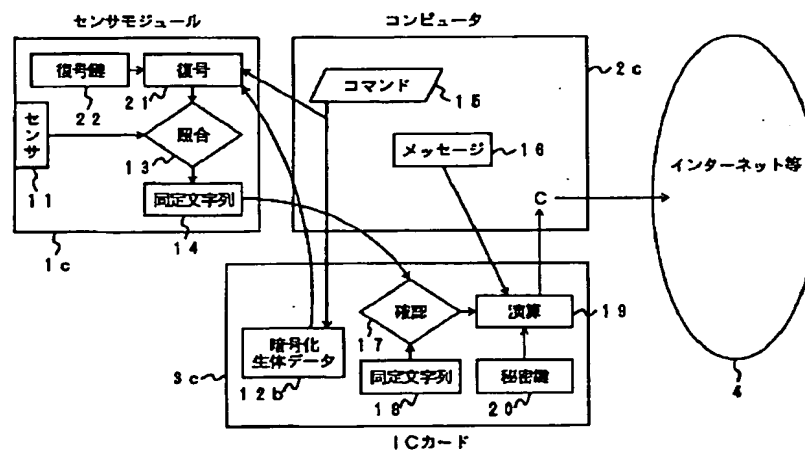
【図4】



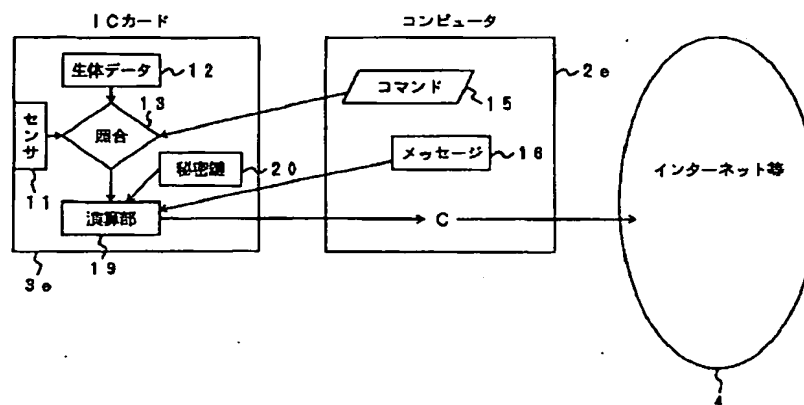
【図3】



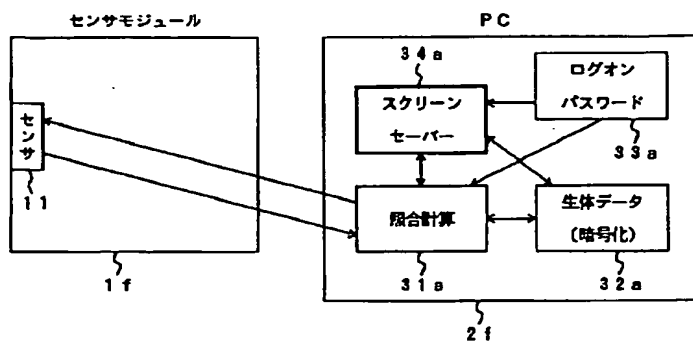
【図5】



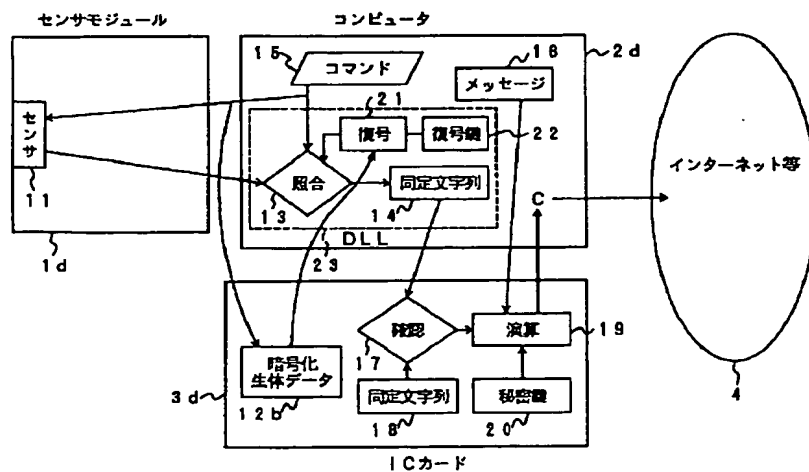
【図9】



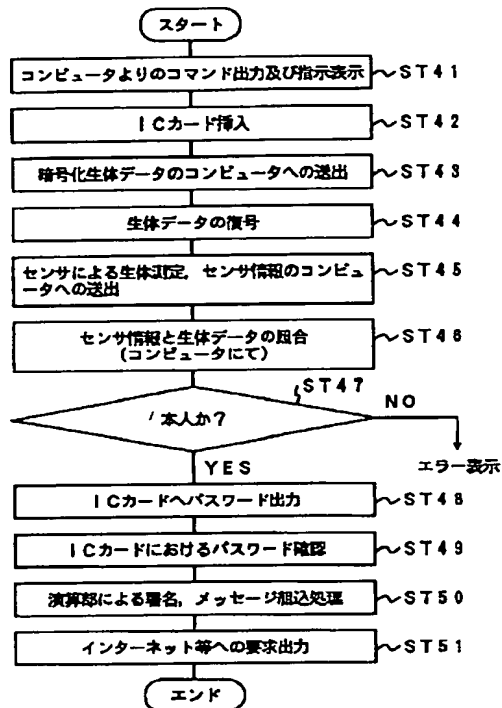
【圖 10】



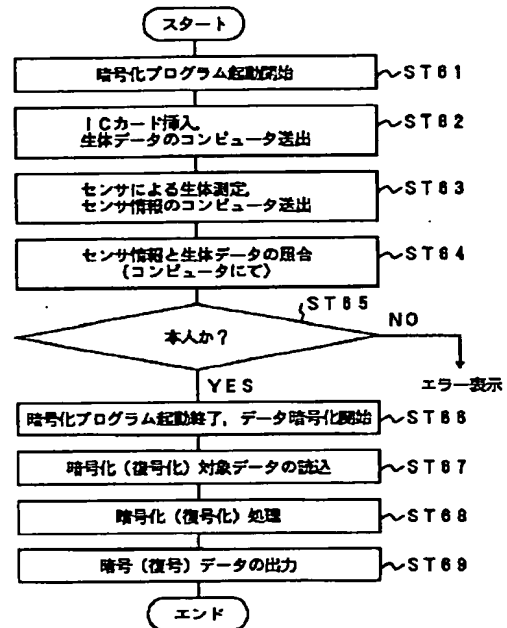
【圖 7】



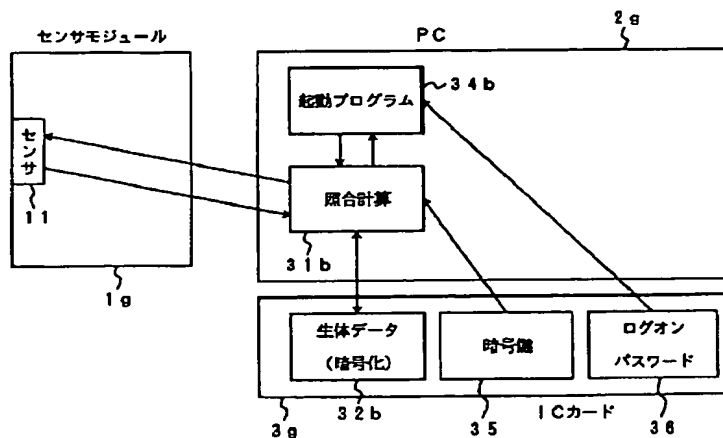
【図8】



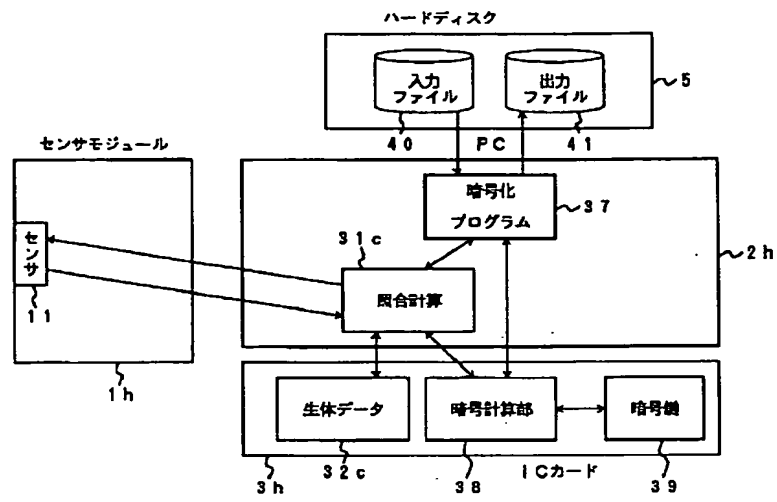
【図13】



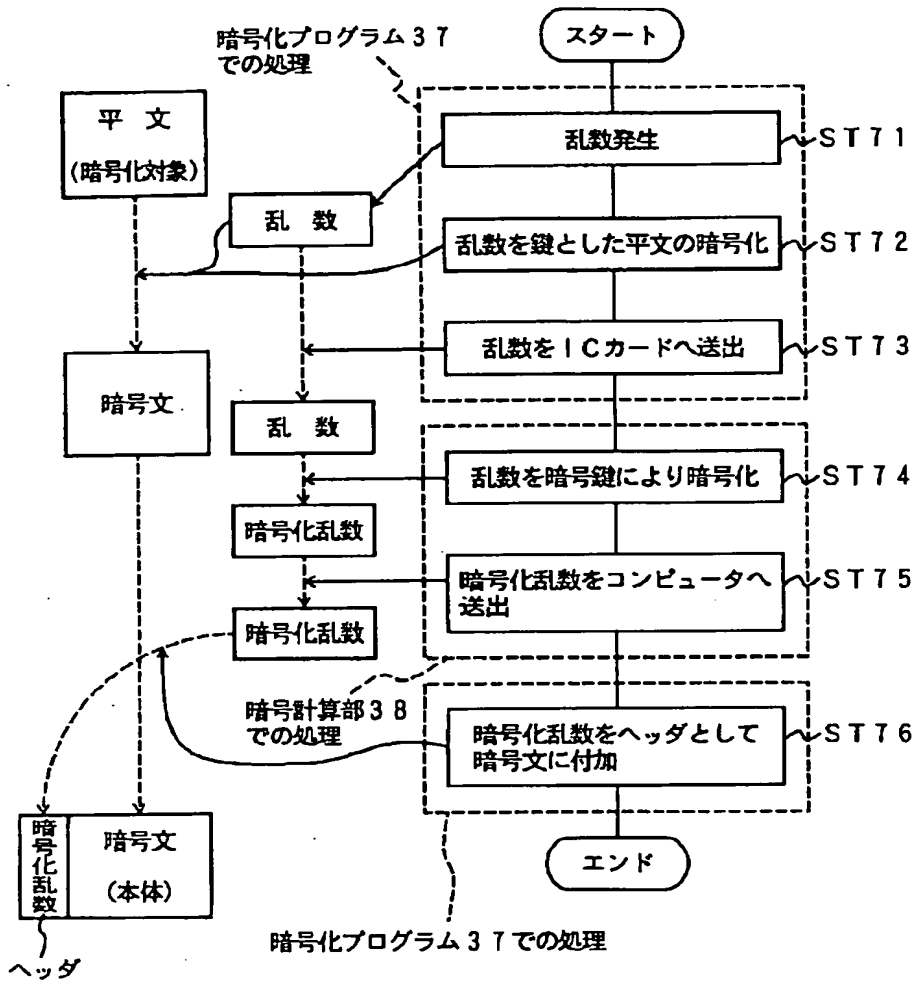
【図11】



【図12】



【圖 14】



【図15】

	候補システム	ICカード	センサ	PC&R/W	サーバー	照合装置のタイプ	備考
第5実施形態	ICカード一体型	生体、照合				1チップ	理想的
第1実施形態	耐タンパーモジュール一体型	PIN	PIN, 生体、照合			1チップ, スタンドアロン	従来カード利用可
第2実施形態	万能ICカード型	生体、照合				従来型	準理想的
第3実施形態	ICカードにデータセンサ計算型	生体	照合			スタンドアロン	一般的、カードに機能付加要
第4実施形態	ICカードにデータ-PC計算型	生体、文字列		文字列、照合		従来型	一般的、カードに機能付加要、依頼計算の検討要
	(参考例1)	生体			照合	従来型	一般的、カードに機能付加要
	(参考例2)		生体	照合		メモリ内蔵型	変形例、従来カード利用可
	(参考例3)		生体		照合	メモリ内蔵型	変形例、従来カード利用可
	(参考例4)	照合	生体			メモリ内蔵型	変形例
	(参考例5)				生体、照合	従来型	従来カード利用可
	(参考例6)			生体(暗号化)、照合		従来型	従来カード利用可

生体データと照合計算の配置可能性